

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 24-CV-21104-RAR

**BENESSERE INVESTMENT
GROUP, LLC, et al.,**

Plaintiffs,

v.

ERIC SWIDER, et al.,

Defendants.

/

ORDER GRANTING IN PART DEFENDANTS' MOTION TO DISMISS

THIS CAUSE is before the Court upon Defendants' Motion to Dismiss Plaintiffs' Complaint ("Motion"), [ECF No. 19], filed on June 17, 2024. The Court has reviewed the Motion; Plaintiffs' Complaint ("Complaint"), [ECF No. 1]; Plaintiffs' Response in Opposition to the Motion ("Response"), [ECF No. 27]; and Defendants' Reply in Support of the Motion ("Reply"), [ECF No. 30]. For the reasons discussed below, it is hereby

ORDERED AND ADJUDGED that Defendant's Motion to Dismiss, [ECF No. 19], is
GRANTED IN PART.

BACKGROUND

I. Factual Background

Plaintiffs Benessere Investment Group ("Benessere") and ARC Global Investments II, LLC ("ARC II") bring this ten-count Complaint under federal and Florida state law against Defendants Eric Swider, Alexander Cano, and Renatus Advisors, LLC ("Renatus"). The facts underlying the Complaint center around Digital World Acquisition Corporation ("DWAC"), a publicly-traded Special Purpose Acquisition Company ("SPAC"), that was poised to merge with Trump Media & Technology Group Corp. ("Trump Media") at the time Plaintiffs brought this

action. Plaintiffs allege that Defendants engaged in a computer hacking scheme aimed at “seiz[ing] control of and enlarg[ing] their holdings in” DWAC. Compl. ¶ 1.

A. SPAC Transactions

A SPAC is a type of company formed to acquire an existing private target company. *Id.* ¶ 11. A SPAC is initially formed as a private company funded by individuals or organizations called “sponsors.” *Id.* ¶ 13. The sponsor ordinarily controls the SPAC by selecting the SPAC’s officers and directors, who “typically overlap with the individuals who own and created the sponsor.” Michael Klausner, Michael Ohlrogge & Emily Ruan, *A Sober Look at SPACs*, 39 Yale J. on Regul. 228, 236 (2022).

SPACs raise funds for the purpose of acquiring a target company by undergoing an initial public offering (“IPO”), turning the SPAC into a publicly-traded company. Compl. ¶ 11. In exchange for their initial investment, the sponsors receive a percentage interest in the SPAC as part of the IPO with the remaining shares offered up to the public. *Id.* ¶ 13.

Following its IPO, a SPAC will typically have up to two years to find a private target company “with which to merge and thereby bring public.” Klausner, et al., *supra*, at 230. The SPAC then acquires “an existing target company either by merger, capital stock exchange, asset acquisition, stock purchase, reorganization, or similar business combination.” Compl. ¶ 11. As a result of this SPAC merger (also called a “de-SPAC transaction”), the target company goes public without enduring the regulatory burden associated with an IPO. See Klausner, et al., *supra*, at 238–39, 238 n.20; *Vogel v. Boris*, No. 20 CIV. 9301 (VM), 2023 WL 5471400, at *1 (S.D.N.Y. Aug. 24, 2023) (SPACs “provide alternative ways for private companies to go public while avoiding the red tape associated with undertaking an . . . [IPO] on their own.”).

B. The Parties' Business Relationships

DWAC formed as a SPAC in December 2020. Compl. ¶ 11. DWAC's sponsor is ARC II, which owns approximately 19% of the interest in DWAC and "maintains a group of investors who . . . provided the seed money to enable DWAC to become publicly traded." *Id.* ¶¶ 14–15. Patrick Orlando, who is not a party to this case, is the managing member of ARC II and also substantially owns and manages Benessere. *Id.* ¶ 3–4. Benessere provides consulting services to ARC II. *Id.* ¶¶ 26.¹ Orlando previously served as DWAC's Chairman and Chief Executive Officer ("CEO") prior to being removed from those positions, and he currently serves as one of DWAC's directors. *Id.* ¶¶ 16, 22. At the time Plaintiffs brought this action, DWAC had entered into a merger agreement with Trump Media, planning to merge "with and into Trump Media" and thereby take Trump Media public through a de-SPAC transaction.² *Id.* ¶ 17.

Defendant Eric Swider is currently the CEO and a Director of DWAC. *Id.* ¶ 6. Swider owns and controls Defendant Renatus. *Id.* Defendant Alexander Cano served as Orlando's assistant at Benessere until January 30, 2023. *Id.* ¶ 7. Following his departure and after Swider became DWAC's CEO, Swider hired Cano as his personal assistant. *Id.* ¶ 27. Cano is currently the President and Secretary of DWAC and is employed as a consultant by Renatus. *Id.* ¶ 7.

¹ The relationship between Benessere and ARC II is somewhat unclear. The Complaint states that Benessere and ARC II are both under the management of Patrick Orlando and that Benessere provides consulting services to ARC II, but does not otherwise specify the relationship between Benessere and ARC II. Compl. ¶¶ 3–4, 26.

² Plaintiffs filed their Complaint on March 21, 2024. At the time the Complaint was filed, DWAC had already entered into a merger agreement with Trump Media on or about October 21, 2021, but had not yet consummated the transaction. See *id.* ¶¶ 6, 17. Shortly after Plaintiffs filed the Complaint, DWAC and Trump Media completed their merger, with Trump Media surviving the merger as a wholly-owned subsidiary of DWAC, which also changed its name to "Trump Media & Technology Group Corp." *Id.* ¶ 17; Motion at 1, n.1. Because the events that form the basis of the Complaint occurred prior to this merger, the Court refers to DWAC and Trump Media as separate entities.

C. The Alleged Hacking Scheme

Plaintiffs allege that Swider, Cano, and Renatus engaged in a hacking scheme aimed at wresting control of ARC II and DWAC away from Patrick Orlando. Swider, then a director of DWAC, devised a scheme “around the first quarter of 2023 . . . to have Orlando ousted as DWAC’s CEO” and to “gain control of ARC II and complete his takeover of the entire DWAC enterprise.” *Id.* ¶¶ 19, 23. The scheme was allegedly designed to benefit himself and his company, Renatus, as Swider “stood to receive massive compensation previously unavailable to him as a director.” *Id.* ¶ 21.

Swider then recruited Cano “to obtain confidential information about ARC II and its investors” by collecting information “held by Beneserre in a protected electronic storage account at Box.com” (“Box”), a website that “offers password-protected storage for computer files.” *Id.* ¶¶ 23–24. The Benessere Box account stores “the lifeblood of Benessere’s business, as well as that of ARC II and other entities for which Benessere provides consulting services.” *Id.* ¶ 26.

Cano “had credentials to access Benessere’s Box Account through his Benessere email account.” *Id.* ¶ 25. Swider knew that Cano had access to the Benessere Box account and promised to make Cano DWAC’s President and to provide Cano with “an outsized compensation package” of DWAC stock (then-valued at over six million dollars) if Cano would help Swider “monitor and access the information in the account.” *Id.* ¶¶ 28–29, 29 n.1.

After leaving Benessere, Cano used his login credentials to access the Box account. *Id.* ¶ 34. Since February 1, 2023, Cano “repeatedly accessed the Box account” to obtain confidential information regarding ARC II’s “investors as well as all financial and other confidential information not only of ARC II but also of Benessere,” which Cano “immediately provided” to Swider. *Id.* ¶¶ 33–35. Cano also “seized total control of the Box [a]ccount as the administrator,” changing the credit card that Box uses to bill for the account to a card not under Orlando’s control,

locking Orlando out of the Box account. *Id.* ¶¶ 30, 40. Cano also granted Swider “collaborator” or “editor” access to a number of files stored in the Box account, allowing Swider to “edit, delete, upload, and download files from the Box Account.” *Id.* ¶¶ 35–37. Cano gave Swider access to at least two files containing access credentials to several accounts belonging to Orlando and/or Benessere, including websites and document repositories such as Quickbooks, Benessere email accounts, MailChimp, and DocuSign, among others. *Id.* ¶¶ 38–39.

Swider and Cano used the information collected from the Box account to send emails to ARC II’s members and investors, consisting of (1) an email on March 5, 2024, sent through Benessere’s MailChimp account, attempting to convince ARC II’s members to remove Orlando as ARC II’s managing member; (2) an email on March 21, 2024, sent through DocuSign, requesting that ARC II investors decide on whether to convert their convertible notes in ARC II into Trump Media shares or cash upon completion of the merger; and (3) an email on March 21, 2024, sent through DocuSign, claiming that ARC II’s members and investors needed to sign a document to elect to convert their convertible notes and vote in favor of the merger. *Id.* ¶¶ 41–46; 56.

Orlando discovered that he had been locked out of the Box account “[a]t some point in 2023.” *Id.* ¶ 30. Orlando demanded that Cano restore his access to the Box account but did not realize then that Cano was continuing to access files in the Box account. *Id.* ¶ 31. Cano restored Orlando’s access “months later,” at which point Orlando became aware of Cano’s and Swider’s access to the Box account. On March 20, 2024, Benessere retained a computer forensics expert to investigate Cano’s and Swider’s access and regain control of Benessere’s accounts, spending “at least \$6,000 on its computer forensics expert’s efforts[.]” *Id.* ¶¶ 47–48. As of the filing of the Complaint, Swider and Cano continued to have access to the Box account and Cano continued to have access to his Benessere email account. *Id.* ¶¶ 49–51.

LEGAL STANDARD

“To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Twombly*, 550 U.S. at 556). Although a complaint need not advance “detailed factual allegation[s],” it must allege more than “labels and conclusions” and offer more than a mere recitation of the elements of a cause of action. *Twombly*, 550 U.S. at 555. “[T]he standard ‘calls for enough fact to raise a reasonable expectation that discovery will reveal evidence’ of the claim.” *Am. Dental Ass’n v. Cigna Corp.*, 605 F.3d 1283, 1289 (11th Cir. 2010) (quoting *Twombly*, 550 U.S. at 556).

“[W]hen plaintiffs ‘have not nudged their claims across the line from conceivable to plausible, their complaint must be dismissed.’” *Id.* (quoting *Twombly*, 550 U.S. at 570). Further, when evaluating a Rule 12(b)(6) motion to dismiss, the court must accept all well-pleaded factual allegations as true and draw all inferences in favor of the plaintiff. *Smith v. United States*, 873 F.3d 1348, 1351 (11th Cir. 2017). The “court must limit its consideration to the pleadings and exhibits attached to the pleadings.” *Gubanova v. Miami Beach Owner, LLC*, No. 12-22319, 2013 WL 6229142, at *1 (S.D. Fla. Dec. 2, 2013) (citing *Chaparro v. Carnival Corp.*, 693 F.3d 1333, 1337 (11th Cir. 2012)).

ANALYSIS

I. Count I – Federal Wiretap Act

Count I of the Complaint, brought by all Plaintiffs against all Defendants, alleges that Defendants “intentionally intercepted or endeavored to intercept the contents of Plaintiffs’ wire,

oral, or electronic communications by surreptitiously hacking into and monitoring the Box Account, Benessere’s email systems, and other Benessere computer systems,” in violation of the Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 (“Wiretap Act”), 18 U.S.C. §§ 2510–2523. Compl. ¶¶ 69–70.

The Wiretap Act creates a private cause of action against a person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a); *id.* § 2520(a) (creating private cause of action). The Wiretap Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” *Id.* § 2510(4). Thus, in order to state a claim under the Wiretap Act, Plaintiffs must show that Defendants “(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device.” *Schwartz v. ADP, Inc.*, No. 2:21-CV-283-SPC-MRM, 2021 WL 3172029, at *3 (M.D. Fla. July 26, 2021) (quoting *Hamilton Grp. Funding, Inc. v. Basel*, 311 F. Supp. 3d 1307, 1314 (S.D. Fla. 2018)).

The Eleventh Circuit applies a “narrow reading” of what constitutes an “interception” under the Wiretap Act. *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003). Under Eleventh Circuit precedent, in order to demonstrate an interception under the Wiretap Act, a plaintiff must show “contemporaneous acquisition of electronic communications while in flight.” *Id.* (finding that acquisition of electronic information stored on a personal computer using a computer virus was not an interception). That is, “an interception of electronic communications must occur contemporaneously with their transmission.” *United States v. Barrington*, 648 F.3d 1178, 1202 (11th Cir. 2011). The corollary of this interpretation is that the term “intercept” will generally not “apply to ‘electronic communications’ when those communications are in ‘electronic

storage.”” *Steiger*, 318 F.3d at 1048 (quoting *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994)). And, as courts throughout this circuit and across the country have found, “unauthorized access to an email account, standing alone, does not constitute interception.” *Bruce v. McDonald*, No. 3:13CV221-MHT, 2014 WL 931522, at *5 (M.D. Ala. Mar. 10, 2014) (collecting cases).

Plaintiffs do not allege facts demonstrating that Defendants “intercepted” any electronic communication contemporaneously with transmission.³ Plaintiffs variously allege that (1) “Defendants used their unauthorized access to the Box Account to acquire Plaintiffs’ electronic communications contemporaneously with their transmission to the Box Account”; (2) “once a document was stored in a shared folder, Box.com contemporaneously transmitted copies to the Defendants’ computers and other linked devices”; (3) Defendants “intentionally intercepted or endeavored to intercept the contents of Plaintiffs’ wire, oral, or electronic communications by surreptitiously hacking into and monitoring the Box Account, Benessere’s email systems, and other Benessere computer systems[]”; and (4) “Defendants’ actions were done contemporaneously with Plaintiffs sending and receiving . . . [electronic] communications.” Compl. ¶¶ 64–65, 73.

These bare allegations are entirely conclusory and contradicted by Plaintiffs’ own account of the facts. Plaintiffs themselves describe Box as “a website that offers password-protected *storage* for computer files” and “a cloud *storage* service that allows users to store date [sic] on its computers by transmitting the information over the internet.” *Id.* ¶¶ 24, 81 (emphasis added). In another count of the Complaint, Plaintiffs allege that “Defendants . . . obtained . . . access to electronic communications *while they are in electronic storage . . .*” *Id.* ¶ 98 (emphasis added).

³ Defendants also argue that Plaintiffs’ Wiretap Act claim should be dismissed because it does not properly allege that Defendants used a “device,” as that term is defined under the Wiretap Act, to intercept the electronic communications. Mot. at 8–9. The Court need not address this argument. The Wiretap Act claim fails on its face because it does not properly allege an interception contemporaneous with transmission.

Nor do Plaintiffs set forth any factual allegations whatsoever suggesting that Defendants intercepted Plaintiffs' emails contemporaneously with transmission.

Plaintiffs attempt to rescue their Wiretap Act claim by recasting Defendants' alleged access to information stored on Box and various email servers as involving transmissions. *See, e.g.*, Response at 7 (alleging that "once a document was stored in a shared folder, Box.com contemporaneously transmitted copies to the Defendants' computers and other linked devices.") (quoting Compl. ¶¶ 64-65). This argument is unavailing. Even accepting that Box is capable of transmitting data between users, the allegations plainly do not show that any interception occurred contemporaneously with transmission. Any access to a file placed in a shared folder would have occurred after the file had already been transmitted. This is not enough to show interception under the Wiretap Act. *See Bruce*, 2014 WL 931522, at *4 (finding that access to another's emails using stolen credentials immediately after the email is sent is not an interception under the Wiretap Act).

Thus, although Plaintiffs may plausibly allege that Defendants accessed stored electronic communications without authorization, they adduce no facts to suggest that any electronic communications were intercepted contemporaneously with their transmission. Indeed, Plaintiffs' Wiretap Act claims appear to be directly at odds with Plaintiff's claim under the Stored Communications Act ("SCA"), which concerns access to an "electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a)(1). Although it is not impossible that a plaintiff could simultaneously maintain claims under the SCA and the Wiretap Act, here, Plaintiff does so for the exact same conduct, effectively claiming that electronic communications at issue in this case were accessed *both* while they were in electronic storage (for the SCA claim) *and* contemporaneously with transmission (for the Wiretap Act claim) *at the same time*. This is plainly

contradictory. On the facts as alleged, Plaintiff does not and cannot state a claim under the Wiretap Act. Accordingly, Count I is due to be dismissed *with prejudice*.⁴

II. Count II – Florida Security of Communications Act

Count II of the Complaint, brought by all Plaintiffs against all Defendants, alleges that Defendants “intentionally intercepted . . . private communications between Plaintiffs, . . . without first obtaining Plaintiffs’ consent,” in violation of the Florida Security of Communication Act (“FSCA”), Fla. Stat. § 934.10. Compl. ¶¶ 75-79.

Florida modeled the FSCA after the Wiretap Act, *see Minotty v. Baudo*, 42 So. 3d 824, 831 (Fla. 4th DCA 2010), and the causes of action under each are essentially identical, *see also* Fla. Stat. Ann. § 934.1 (creating civil cause of action for “[a]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of” the FSCA); *see also* 18 U.S.C. § 2520(a) (creating civil cause of action for “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of” the Wiretap Act). Given the similarities between the two statutes, “Florida follows federal courts as to the meaning of provisions after which Chapter 934 was modeled.” *Minotty*, 42 So. 3d at 831 (citing *O’Brien v. O’Brien*, 899 So. 2d 1133, 1135–36 (Fla. 5th DCA 2005)).

Accordingly, the FSCA, like the Wiretap Act, “does not provide a cause of action to those whose electronic communications were acquired from electronic storage rather than intercepted

⁴ The Court notes that Plaintiffs requested leave to amend in their Response. *See* Response at 19–20. “If the underlying facts or circumstances relied upon by a plaintiff may be a proper subject of relief,” *Foman v. Davis*, 371 U.S. 178, 182 (1962), leave to amend “should be freely given,” Fed. R. Civ. P. 15(a). Here, however, the Court finds that leave to amend would be futile because the underlying facts and circumstances cannot support a claim for relief under the Wiretap Act and contradict Plaintiff’s claims under the SCA, which survive the instant Motion to Dismiss. *See Hall v. United Ins. Co. of Am.*, 367 F.3d 1255, 1263 (11th Cir. 2004) (“[A] district court may properly deny leave to amend the complaint under Rule 15(a) when such amendment would be futile.”). Further, the Complaint offers the Court no reason to believe that Plaintiffs “could offer sufficient allegations to make a claim for relief plausible on its face.” *Patel v. Georgia Dep’t BHDD*, 485 F. App’x 982, 983 (11th Cir. 2012) (affirming district court’s decision to deny leave to amend where the plaintiff failed to provide any facts that could support the underlying claims in the complaint). Accordingly, the Court dismisses Plaintiff’s Wiretap Act claim without leave to amend.

during contemporaneous transmission.” *Handley v. Wilson*, No. 08-14444, 2010 WL 11607357, at *9 (S.D. Fla. Feb. 10, 2010); *Schwartz*, 2021 WL 3172029, at *4 (citing *Handley*, 2010 WL 11607357, at *8–9); *Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 WL 3087860, at *3 n.3, *6 (Fla. 11th Cir. Ct. June 17, 2021) (noting that the FSCA’s definition of “intercept” is identical to the Wiretap Act’s corresponding definition and applying the Wiretap Act’s definition to FSCA). Therefore, for the same reasons explained with regard to Count I, Count II is due to be dismissed *with prejudice*.

III. Count III – Federal Computer Fraud and Abuse Act

Count III of the Complaint, brought by Benessere against all Defendants, alleges that Defendants violated several provisions of the Federal Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030. *See* Compl. ¶¶ 80–88.

The CFAA creates a private cause of action for violations of the CFAA “only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).” 18 U.S.C. § 1030(g). Applicable here, Subclause I permits a civil action only if the plaintiff demonstrates economic loss “aggregating at least \$5,000 in value” during “any 1-year period.” 18 U.S.C. § 1030(c)(4)(A)(i)(I). Count III argues that Defendants violated three separate provisions of the CFAA: (1) 18 U.S.C. § 1030(a)(2)(C), which creates liability for whoever “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer”; (2) 18 U.S.C. § 1030(a)(4), which creates liability for whoever “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period”; and (3) 18 U.S.C. § 1030(a)(5)(C), which creates liability for whoever “intentionally

accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.”⁵

Defendants seek dismissal of the CFAA claims on the grounds that they are brought as a shotgun pleading.⁶ Mot. at 11–13. The Court agrees. “The unifying characteristic of all types of shotgun pleadings is that they fail to one degree or another, and in one way or another, to give the defendants adequate notice of the claims against them and the grounds upon which each claim rests.” *See Weiland v. Palm Beach Cty. Sheriff’s Office*, 792 F.3d 1313, 1321–23 (11th Cir. 2015). The Eleventh Circuit has identified “four rough types” or categories of shotgun pleadings: (1) “a complaint containing multiple counts where each count adopts the allegations of all preceding counts”; (2) a complaint that contains “conclusory, vague, and immaterial facts not obviously connected to any particular cause of action”; (3) a complaint that fails to “separat[e] into a different count each cause of action or claim for relief”; and (4) a complaint that “assert[s] multiple claims against multiple defendants without specifying which of the defendants are responsible for which

⁵ The CFAA defines a “computer” to include “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.” 18 U.S.C. § 1030(e)(1). The CFAA defines a “protected computer” to include “a computer . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.” 18 U.S.C. § 1030(e)(2)(B). The parties do not dispute at this stage whether Defendants accessed one or more “protected computers.”

⁶ Defendants also argue that Benessere has not demonstrated over \$5,000 in losses, as required by the CFAA, because Benessere does not describe the loss for each of the three protected computers it alleges Defendants accessed. Mot. at 12–13. But the CFAA requires economic loss “aggregating at least \$5,000 in value,” which may be combined across multiple computers or users when the loss stems from a single act. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (emphasis added); *see In re Am. Online, Inc.*, 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001) (injuries stemming from a single act may be aggregated under the CFAA for purposes of meeting the CFAA loss threshold). Plaintiffs plausibly allege that Cano’s continued retention and sharing of access to the accounts caused Plaintiffs to suffer losses of at least \$6,000 on its computer forensics expert’s efforts to remediate the alleged hacking. Compl. ¶ 48. This is plainly enough to meet the CFAA loss threshold.

acts or omissions, or which of the defendants the claim is brought against.” *See id.* (citations omitted).

The Court agrees with Defendants that Benessere’s CFAA claims display signature elements of a shotgun pleading. *See Mot.* at 11–13. Count III starts by reincorporating all facts asserted in paragraphs 1–60 of the Complaint. Compl. ¶ 80. It follows by providing three paragraphs reciting the elements of each of the three CFAA claims without specifying what facts alleged meet each element of the respective claims. *See Compl.* ¶ 83 (“From January 31, 2023 onward, Defendants intentionally and continually accessed Benessere’s computer systems covertly to obtain confidential and proprietary information in violation of 18 U.S.C. § 1030(a)(2)(C).”); *id.* ¶ 84 (“From January 31, 2023 onward, Defendants knowingly and with intent to defraud accessed Benessere’s computer systems covertly to further the intended fraud and obtain valuable property for the benefit of Defendants in violation of 18 U.S.C. § 1030(a)(4).”); *id.* ¶ 85 (“From January 31, 2023 onward, Defendants intentionally accessed Benessere’s computer systems covertly, and as a result of such conduct, caused damage and loss, in violation of 18 U.S.C. § 1030(a)(5)(C).”). There is also some confusion in Count III as to which Plaintiffs are allegedly responsible for the actions underlying the CFAA claims. Although the heading of Count III is styled as being advanced “by Benessere against All Defendants,” Compl. at 13, this count later asserts that *all* “Plaintiffs are entitled” to relief under the CFAA, *id.* ¶ 88.

Although it is possible that the facts as pleaded could support at least some of the elements of the CFAA claims, these defects make it exceedingly difficult to discern which Defendant is alleged to be responsible for what action and what particular facts support each of the distinct elements of the three separate CFAA theories squeezed into Count III. It is not the Court’s duty to rummage through a haystack of facts looking for a needle. *See Pouyeh v. Pub. Health Tr. of Jackson Health Sys.*, 832 F. App’x 616, 623 (11th Cir. 2020) (Rule 8 “aims . . . to permit the court

to determine which facts are intended to support which claims”) (citing *Weiland*, 792 F.3d at 1320); *Shillingford v. Rolly Marine Serv., Inc.*, No. 14-61936, 2014 WL 6682477, at *2 (S.D. Fla. Nov. 25, 2014) (noting it is not the Court’s duty “to search through a plaintiff’s filings to find or construct a pleading that satisfies Rule 8.”) (citations omitted). As the oft-repeated judicial maxim goes, “[j]udges are not like pigs, hunting for truffles buried in briefs.” *Gomez v. City of Miami*, 696 F. Supp. 3d 1176, 1188 n.5 (S.D. Fla. 2023) (quoting *United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir. 1991)). Accordingly, Count III is due to be dismissed as a shotgun pleading.

IV. Count IV – Florida Computer Abuse and Data Recovery Act

Count IV of the Complaint, brought by Benessere against all Defendants, alleges that Defendants violated several provisions of the Florida Computer Abuse and Data Recovery Act (“CADRA”), Fla. Stat. §§ 668.801–805. *See* Compl. ¶¶ 89–94. Specifically, Count IV alleges that Defendants violated two CADRA provisions that respectively create private causes of action against anyone who “knowingly and with intent to cause harm or loss” either “[o]btains information from a protected computer without authorization and, as a result, causes harm or loss[,]” *id.* § 668.803(1), or “[c]auses the transmission of a program, code, or command to a protected computer without authorization and, as a result of the transmission, causes harm or loss[.]” *id.* § 668.803(2).

Plaintiffs’ CADRA claims follow the same shotgun formula as the CFAA claims, reasserting all allegations of the Complaint, Compl. ¶ 89, and reciting the elements of the two separate statutory claims, *id.* ¶¶ 91, 93. Like the CFAA claims, the CADRA claims jumble which Defendants are allegedly responsible for the conduct at issue. *Compare id.* at 14 (styling Count IV as “by Benessere against All Defendants”) (emphasis omitted) *with id.* ¶¶ 91, 93–94 (alleging

that Defendants caused “Plaintiffs” harm). Accordingly, Count IV is due to be dismissed as a shotgun pleading.⁷

V. Count V – Electronic Stored Communications Act

Count V, brought by Benessere against all Defendants, alleges that Defendants violated the Electronic Stored Communications Act (“SCA”), which, in relevant part, creates a civil cause of action against anyone who “intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.” 18 U.S.C. § 2701(a)(1); *id.* § 2707(a) (creating private cause of action). There are thus five elements of an SCA claim: “(1) access without authorization or exceeding an authorization to access (2) a facility (3) that provides an electronic communication service (4) thereby obtaining a wire or electronic communication (5) while the communication is in electronic storage.” *Trump v. Clinton*, 626 F. Supp. 3d 1264, 1316 (S.D. Fla. 2022) (cleaned up). Benessere alleges that Defendants’ unauthorized access to the Box account and to Benessere’s Office 365 email accounts violates the SCA. Compl. ¶¶ 95–99.

Defendants argue that the SCA claims should be dismissed because Benessere does not adequately allege that Box is a facility that provides an “electronic communication service” under the SCA. Mot. at 14–15. The SCA does not define the term “facility.” The SCA defines an “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). An “electronic

⁷ Defendants separately argue that the entire Complaint should be dismissed as a shotgun pleading. Mot. at 4–5. Although the Court agrees the Complaint is not a model of clarity, it is not a shotgun pleading in its entirety. Defendants prove themselves more than capable of addressing the merits of Plaintiffs’ allegations in their Motion to Dismiss and Reply. Accordingly, with the exception of Counts III and IV, the Complaint does not fail to give each Defendant “adequate notice of the claims against them and the grounds upon which each claim rests.” *Weiland*, 792 F.3d at 1323.

“communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” *Id.* § 2510(13). And “electronic storage” means “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,” as well as “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” *Id.* § 2510(17).

Applying these definitions, federal courts have generally found the SCA “to encompass only traditional ‘electronic communications services’ such as internet service providers, electronic mail providers, telecommunications companies, and remote computing services.” *IPC Sys., Inc. v. Garrigan*, No. 11-3910, 2012 WL 12872028, at *9 (N.D. Ga. May 21, 2012) (collecting cases); *see also Steiger*, 318 F.3d at 1049 (noting that “the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS).”). The Eleventh Circuit has also found that a cloud-based email provider can provide electronic communication services. *Brown Jordan Int'l, Inc. v. Carmicle*, 846 F.3d 1167, 1177 n.4 (11th Cir. 2017); *Trump*, 62 F. Supp. 3d at 1317 (finding that Microsoft Office 365, “a cloud-based service . . . [that] provides the ability to send and receive emails . . . is a facility through which an electronic communication service is provided.”).

Defendants argue that Box is not an “electronic communication service” because “Benessere does not allege that the Box Account had the ability to send or receive wire or electronic communications[,]” Mot. at 15 (citing Compl. ¶ 24), and the Complaint characterizes Box as a storage service, Reply at 7.

There is little clear authority addressing whether a cloud-based provider of electronic storage services can be a provider of electronic communication services within the meaning of the

SCA.⁸ A handful of federal courts have found at the motion to dismiss stage that Dropbox or other cloud-based providers of electronic storage services allegedly analogous to Box, *see Response at 12*, are providers of electronic communication services—at least where a plaintiff alleges that the cloud-based service provided communications functionality. *See TLS Mgmt. v. Rodriguez-Toledo*, 260 F. Supp. 3d 154, 160–161 (D.P.R. 2016) (denying motion to dismiss where plaintiff alleged that Dropbox “transmit[s] a copy of the file to the [user’s] computer; that a user can also use automatic transmission through shared folders; and that documents placed in shared folders are instantly transmitted from a [user’s] computer to the cloud.”) (internal quotation marks omitted); *Lane v. Brocq*, No. 15 C 6177, 2016 WL 1271051, at *6 (N.D. Ill. Mar. 28, 2016) (denying motion to dismiss where plaintiffs alleged “that Defendant accessed electronic files stored on cloud-based servers[, including Dropbox,] that were connected to the internet.”); *see also William Gottlieb Mgmt. Co., LLC v. Carlin*, No. 20 CIV. 08907, 2024 WL 1311854, at *5 (S.D.N.Y. Mar. 26, 2024) (denying motion to dismiss SCA claims based on defendant’s unauthorized access to plaintiff’s Dropbox account without analyzing whether Dropbox provides electronic communications services); *cf. Billiter v. SP Plus Corp.*, 329 F. Supp. 3d 459, 470 (M.D. Tenn. 2018) (declining to decide whether the SCA applies to Dropbox at the summary judgment stage where plaintiff failed to allege facts relevant to whether the SCA applies to Dropbox). However, at least one court in this Circuit has found that a service provider that *only* offers cloud-based *storage* services—i.e., without allegations that the service also had *communications* functionality—does not provide electronic communication services within the meaning of the SCA. *See St. Johns Vein Ctr., Inc. v. StreamlineMD LLC*, 347 F. Supp. 3d 1047, 1065 (M.D. Fla. 2018) (granting motion to dismiss where plaintiff’s allegations tended to show that a cloud-based medical database was primarily

⁸ To the Court’s knowledge, there is no case analyzing whether a Box account qualifies as a provider of electronic communication services.

related to the “electronic access and use of information, rather than the transmission or receipt of information.”).

At the motion to dismiss stage, Benessere has met its burden of showing that Box provides an electronic communications service. Similar to the plaintiffs in *TLS* and *Lane*, Benessere alleges that Box allows users to transmit data through shared folders that transmit electronic communications between users over the internet in the form of files. See Compl. ¶ 65 (“[O]nce a document was stored in a shared folder, Box.com contemporaneously transmitted copies to the Defendants’ computers and other linked devices.”); *id.* ¶ 81 (“Box.com is a cloud storage service that allows users to store date [sic] on its computers by transmitting the information over the internet[.]”).

The task for the Court at this stage is not to determine definitively whether Box is an “electronic communications service,” but whether Benessere plausibly alleges that it is. Drawing all inferences in favor of Benessere, Benessere has done so. Accordingly, Defendant’s request to dismiss Count V is denied.

VI. Count VI – Tortious Interference with Business Relations

Count VI, brought by Benessere against all Defendants, alleges that Defendants tortiously interfered with ARC II’s business relationships with its investors. Compl. ¶¶ 100–103.

Under Florida law, a claim for tortious interference with business relations has four elements: (1) “the existence of a business relationship, not necessarily evidenced by an enforceable contract”; (2) “knowledge of the relationship on the part of the defendant”; (3) “an intentional and unjustified interference with that relationship by the defendant”; and (4) “damage to the plaintiff as a result of the breach of the relationship.” *Kenniasty v. Bionetics Corp.*, 82 So. 3d 1071, 1074 (Fla. 5th DCA 2011) (quoting *Magre v. Charles*, 729 So. 2d 440, 443–44 (Fla. 5th DCA 1999)).

Benessere's claim fails because it does not allege any interference by Defendants with *Benessere's* business relations. Count VI is clearly styled as "by Benessere against All Defendants," Compl. at 15, and the first paragraph of Count VI states that "Plaintiff Benessere realleges" the factual content of the Complaint, *id.* ¶ 100. But all of Benessere's allegations in Count VI relate to Defendants' alleged interference with *ARC II's* business relations with its own investors. See *id.* ¶ 101 (alleging that Defendants "used the information improperly obtained from the Box Account to contact ARC II's investors in an effort to knowingly interfere with ARC II's business relationships with such investors."); *id.* ¶ 102 ("Defendants were aware of ARC II's business relationships with the investors and caused harm to such relationships for which ARC II has suffered damages."). Because Count VI does not allege *any* interference with Benessere's business relationships, it fails on its face, and is due to be dismissed.

VII. Count VII – Tortious Interference with Contract

Count VII, brought by ARC II against all Defendants, alleges that Defendants tortiously interfered with ARC II's contractual relationships with its investors. Compl. ¶¶ 104–110.

Under Florida law, a claim for tortious interference with contract has four elements: (1) "the existence of a . . . contract"; (2) "knowledge of the . . . contract on the part of the defendant"; (3) "procurement of the contract's breach"; and (4) "damage to the plaintiff" resulting from the breach. *Howard v. Murray*, 184 So. 3d 1155, 1166 (Fla. 1st DCA 2015). "The gravamen of an action for tortious interference with a contractual relationship is the malicious interference by a third party, with a contract between other persons, whereby one contracting party is induced to breach the contract to the injury of the other." *McKinney-Green, Inc. v. Davis*, 606 So. 2d 393, 397 (Fla. 1st DCA 1992) (citations omitted). Thus, "in an action for tortious interference with a contract, a plaintiff must demonstrate there was a breach of contract." *Novell v. Bank of Am. Corp.*, No. 14-80672, 2014 WL 7564678, at *4 (S.D. Fla. Dec. 3, 2014) (citing *Chicago Title Ins. Co. v.*

Alday-Donalson Title Co. of Fla., Inc., 832 So. 2d 810, 814 (Fla. 2d DCA 2002) (distinguishing the elements of tortious interference with contract from those of tortious interference with business relations); *see also In re Jan. 2021 Short Squeeze Trading Litig.*, 584 F. Supp. 3d 1161, 1200 (S.D. Fla. 2022), *aff'd*, 76 F.4th 1335 (11th Cir. 2023) (“Florida law requires showing that the defendant caused a breach of contract[]” in order to demonstrate tortious interference with contract); *accord Farah v. Canada*, 740 So. 2d 560, 561–562 (Fla. 5th DCA 1999).

ARC II’s claim fails because it does not allege that Defendants procured the breach of any contract between ARC II and its investors. Indeed, ARC II does not point to any specific contract or contractual provision that Defendants induced ARC II’s investors to breach. ARC II alleges only that Defendants “used the information improperly obtained from the Box Account to contact ARC II’s investors in an effort to knowingly interfere with ARC II’s contractual relationships with such investors[,]” and thereby “caused harm to such relationships for which ARC II has suffered damages.” Compl. ¶¶ 107–108. But ARC II does not allege that Defendants induced any investors to breach their contracts with ARC II, as Florida law demands. Accordingly, Count VII is due to be dismissed.

VIII. Count VIII – Breach of Fiduciary Duty

Count VIII of the Complaint, brought by Benessere against Cano, alleges that Cano breached his “implied fiduciary duties” to Benessere “after Cano no longer was engaged by Benessere.” Compl. ¶ 112. Cano argues that he did not breach any fiduciary duty to Benessere because (1) Cano and Benessere did not have a fiduciary relationship, and (2) even if Cano was a fiduciary, “his fiduciary duties ceased when his employment ended” on January 30, 2023. Mot. at 17–18.

Under Florida law, a claim for breach of fiduciary duty requires a plaintiff to show (1) “existence of a fiduciary duty”; (2) “a breach of that duty”; and (3) “damage proximately

caused by that duty.” *Brouwer v. Wyndham Vacation Resorts, Inc.*, 336 So. 3d 372, 373 (Fla. 5th DCA 2022). “A fiduciary relationship may be either express or implied.” *First Nat. Bank & Tr. Co. of Treasurer Coast v. Pack*, 789 So. 2d 411, 415 (Fla. 4th DCA 2001) (citation omitted). “A fiduciary relationship which is implied in law is based on the specific factual circumstances surrounding the transaction and the relationship of the parties and may be found when confidence is reposed by one party and a trust accepted by the other.” *Id.* (cleaned up).

An implied fiduciary duty may exist between employer and employee when an employee is entrusted with confidential information, and the duty to keep those confidences endures even after the employee has left the employer. *See Sensormatic Elecs. Corp. v. TAG Co. US, LLC*, 632 F. Supp. 2d 1147, 1191 (S.D. Fla. 2008), *aff’d in part sub nom. Sensormatic Elecs., LLC v. Kahle*, 367 F. App’x 143 (Fed. Cir. 2010) (finding breach of implied fiduciary duty when employee was entrusted with confidential information, retained records that contained employer’s confidential information after he left the employer, and then disclosed that confidential information to a competitor). Thus, under Florida law, “an employee may not engage in disloyal acts in anticipation of his future competition, such as using confidential information acquired during the course of his employment” *Furmanite America, Inc. v. T.D. Williamson, Inc.*, 506 F. Supp. 2d 1134, 1149 (M.D. Fla. 2007) (citing *Harllee v. Professional Serv. Indust., Inc.*, 619 So. 2d 298, 300 (Fla. 3d DCA 1992)). An employee does not have to be managerial in order to have this duty. *Id.* (citing *Fish v. Adams*, 401 So. 2d 843, 845 (Fla. 5th DCA 1981)).

Benessere plausibly alleges that Cano owed Benessere a fiduciary duty not to disclose Benessere’s proprietary and confidential information. Benessere alleges that it entrusted Cano with proprietary and confidential information, including by providing Cano with credentials to access the Box account, which contained confidential and sensitive information such as “files containing all information with regard to all investors as well as all financial and other confidential

information not only of ARC II but also of Benessere.” Compl. ¶¶ 25–26, 34, 113. Cano and the other Defendants continue to have access to Benessere’s confidential and proprietary information. *Id.* ¶ 54. Benessere alleges that, in providing Cano with confidential information, it placed “trust and confidence in Cano . . . not [to] disclose, share, or otherwise use any of the property or information he worked with outside of Benessere; . . . and [not to] directly or indirectly divulge to any person any non-public information obtained while performing his duties.” *Id.* ¶ 114. And Cano “accepted the trust and confidence reposed in him by Benessere and assumed the aforementioned fiduciary duties.” Compl. ¶ 115.

Taken together, the allegations plausibly allege that Cano had a fiduciary duty to Benessere by virtue of the confidential information entrusted to him—and breached that duty by retaining said confidential information and disclosing it to Benessere’s competitors. *Sensormatics*, 632 F. Supp. 2d at 1191. Accordingly, Defendant’s request to dismiss Count VIII is denied.

IX. Count IX – Aiding and Abetting Breach of Fiduciary Duty

Count IX of the Complaint, brought by Benessere against Swider and Renatus, alleges that Swider and Renatus are liable for aiding and abetting Cano’s breach of fiduciary duty. Compl. ¶¶ 118-122.

Florida law “recognizes a cause of action for aiding and abetting common law torts, such as breach of fiduciary duty.” *Taubenfeld v. Lasko*, 324 So. 3d 529, 543 (Fla. 4th DCA 2021) (quotation omitted); *see also Fonseca v. Taverna Imports, Inc.*, 212 So. 3d 431, 442 (Fla. 3d DCA 2017) (“Florida law recognizes a cause of action for aiding and abetting the breach of a fiduciary duty.”) (citations omitted). A claim for aiding and abetting the breach of a fiduciary duty requires a plaintiff to show (1) “a fiduciary duty on the part of a primary wrongdoer”; (2) “a breach of that fiduciary duty”; (3) “knowledge of the breach by the alleged aider and abettor”; and (4) “the aider

and abettor's substantial assistance or encouragement of the wrongdoing." *Fonseca*, 212 So. 3d at 442 (citations omitted).

Benessere plausibly alleges that Swider and Renatus aided and abetted Cano's breach of fiduciary duty. Benessere has already established Cano's breach of fiduciary duty, so the only elements for the Court to consider are Swider's and Renatus's knowledge of the breach and whether they substantially assisted or encouraged the breach. The Complaint alleges that Swider enlisted Cano's assistance in obtaining Benessere's confidential information that Cano acquired during the course of his employment. Compl. ¶ 24. Swider then made Cano his personal assistant, and installed him as DWAC's President, for which Cano received a note convertible into 165,000 shares of DWAC stock, then valued at over six million dollars. *Id.* ¶¶ 27–29, 29 n.1. Cano provided Swider with Benessere's confidential information, as well as the ability to edit, delete, upload, and download files from the Box account. *Id.* ¶¶ 35–39. And Swider used this information to oust Orlando as DWAC's CEO "for his own gain and that of Renatus." *Id.* ¶¶ 19, 35.

These allegations plausibly allege that Swider and Renatus had knowledge of Cano's access to Benessere's confidential information acquired during his employment, and therefore also had knowledge of his breach when he provided that confidential information to Swider. The Complaint also plausibly alleges that Swider and Renatus procured Cano's breach by providing him with employment and compensation, thereby substantially assisting and encouraging the breach. Accordingly, Defendant's request to dismiss Count IX is denied.

X. Count X – Civil Conspiracy

Count X of the Complaint, brought by all Plaintiffs against all Defendants, alleges that Cano, Swider, and Renatus engaged in a civil conspiracy "to hack into Benessere's computer systems and use the information contained therein to have Orlando ousted as DWAC's CEO and defame Orlando." *Id.* ¶ 124.

Under Florida law, a claim of civil conspiracy requires a plaintiff to show “(1) an agreement between two or more parties; (2) to do an unlawful act or a lawful act by unlawful means; (3) the execution of some overt act in pursuance of the conspiracy; and (4) damage to the plaintiff as a result of said acts.” *Logan v. Morgan, Lewis & Bockius LLP*, 350 So. 3d 404, 412 (Fla. 2d DCA 2022). A civil conspiracy “is not a separate or independent tort[,] but is a vehicle for imputing the tortious acts of one coconspirator to another to establish joint and several liability.” *Lorillard Tobacco Co. v. Alexander*, 123 So. 3d 67, 80 (Fla. 3d DCA 2013) (quotation omitted). Because Florida “does not recognize civil conspiracy as a freestanding tort,” *Banco de los Trabajadores v. Cortez Moreno*, 237 So. 3d 1127, 1136 (Fla. 3d DCA 2018) (citation omitted), a plaintiff must “identify an actionable underlying tort or wrong” in order to state a claim, *Plastiquim, S.A. v. Odebrecht Constr., Inc.*, 337 So. 3d 1270, 1273 (Fla. 3d DCA 2022).

Here, Plaintiffs allege underlying claims “including, but not limited to violations of” the Wiretap Act, the FSCA, the CFAA, and the CADRA, as well as an unpleaded claim for “tortious interference with Benessere’s business relationships with ARC II.”⁹ Compl. ¶¶ 124–125. However, as the Court has explained above, Plaintiffs fail to state a claim for alleged violations of the Wiretap Act, the FSCA, the CFAA, and the CADRA.

Because Plaintiffs fail to establish any of the underlying claims, the civil conspiracy claim must also fail. *See Alhassid v. Bank of Am., N.A.*, 60 F. Supp. 3d 1302, 1317 (S.D. Fla. 2014) (dismissing civil conspiracy claim where the court also dismissed underlying claims) (citing *Rebman v. Follett Higher Educ. Grp., Inc.*, 575 F. Supp. 2d 1272, 1280 (M.D. Fla. 2008)); *Weisman v. S. Wine & Spirits of Am., Inc.*, 297 So. 3d 646, 652 (Fla. 4th DCA 2020) (same). Accordingly, Count X is due to be dismissed.

⁹ Benessere’s claim for tortious interference with business relations alleges interference with “ARC II’s business relationships with its investors,” Compl. ¶ 101—not “Benessere’s business relationships with ARC II,” *id.* ¶ 125.

XI. Liability of Renatus

Defendants argue in footnotes that Defendant Renatus “is not a proper party to this action” because Plaintiffs “fail to allege how Renatus was involved in any challenged act, instead alleging only that Swider ‘devised this scheme to benefit his company, Renatus Advisors, and himself.’” *See* Motion at 2, n.2; *id.* at 4, n.4 (quoting Compl. ¶¶ 21, 35).

Although the Court notes the dearth of factual allegations in the Complaint regarding Renatus’s involvement beyond allegations that Renatus benefitted from the scheme, the Court declines to consider this argument without proper briefing. It is up to the “discretion of the Court to decide whether to entertain an argument raised only in a footnote.” *Pinchasov v. Robinhood Fin. LLC*, No. 20-24897, 2021 WL 4991159, at *1 (S.D. Fla. Sept. 21, 2021) (citing *Pinson v. JPMorgan Chase Bank, Nat'l Ass'n*, 942 F.3d 1200, 1209 n.5 (11th Cir. 2019); *MSPA Claims I, LLC v. Covington Specialty Ins.*, No. 19-21583, 2021 WL 2915097, at *8 n.8 (S.D. Fla. July 12, 2021)). Generally speaking, “addressing legal arguments in footnotes is an incorrect method to present substantive arguments on the merits or otherwise request relief from the Court.” *Sony Music Ent. v. Vital Pharms., Inc.*, No. 21-22825, 2022 WL 4771858, at *13 (S.D. Fla. Sept. 14, 2022). And there is no need for this Court to address arguments made in a footnote “in a perfunctory manner without supporting arguments and authority.” *U.S. S.E.C. v. Big Apple Consulting USA, Inc.*, 783 F.3d 786, 812 (11th Cir. 2015) (internal quotations omitted).

The Court will not entertain Defendants’ passing argument regarding Renatus’s liability as it is not properly before the Court. An argument buried in a footnote in a motion to dismiss with only cursory elaboration and no cited authority does not provide Plaintiffs with proper notice of Defendants’ argument, nor does it provide the Court with a basis on which to rule.

CONCLUSION

Based on the foregoing, it is hereby **ORDERED AND ADJUDGED** that Defendant's Motion to Dismiss, [ECF No. 19], is **GRANTED IN PART** as follows:

1. Counts I and II are **DISMISSED with prejudice**.
2. Counts III, IV, VI, VII, and X are **DISMISSED without prejudice and with leave to amend**.
3. The Motion to Dismiss is **DENIED** with respect to the remaining Counts.
4. Should Plaintiffs choose to file an amended complaint, they shall do so **on or before November 12, 2024**.
5. Further, the parties shall appear for an in-person status conference on **Wednesday, November 13, 2024, at 10:30 A.M.** Parties shall report to Courtroom 11-2, 11th Floor, at the Wilkie D. Ferguson, Jr. United States Courthouse, 400 North Miami Avenue, Miami, Florida 33128.

DONE AND ORDERED in Miami, Florida, this 31st day of October, 2024.



RODOLFO A. RUIZ II
UNITED STATES DISTRICT JUDGE